



ПОЛОЖЕНИЕ ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ, ДОБРОВОЛЬЦЕВ, КЛИЕНТОВ И КОНТРАГЕНТОВ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Целями настоящего Положения является определение политики в отношении обработки персональных данных работников, добровольцев, клиентов и контрагентов АНО "Новые Перспективы" (далее – «Организация») от несанкционированного доступа, неправомерного их использования или утраты.

1.2. Настоящее Положение разработано в соответствии с Конституцией РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информатизации, информационных технологиях и о защите информации», Постановлениями Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляющей без использования средств автоматизации», иными нормативными актами, действующими на территории Российской Федерации.

1.3. В настоящем Положении используются следующие термины и определения:

Оператор – АНО "Новые Перспективы", вступившая в договорные отношения с работником, добровольцем, клиентом или контрагентом, или оказывающая услуги физическому лицу, юридическому лицу или индивидуальному предпринимателю, или осуществляющая благотворительную деятельность физическому лицу, юридическому лицу или индивидуальному предпринимателю.

Ответственный за ООПД - Ответственный за организацию обработки персональных данных в Организации;

Клиент – физическое лицо, официальный представитель – физическое лицо юридического лица или индивидуального предпринимателя, вступившее в договорные отношения по оказанию услуг с Организацией, либо лицо, в отношении которого Организацией оказываются услуги в рамках благотворительной деятельности.

Контрагент – физическое лицо, представитель – физическое лицо юридического лица и индивидуального предпринимателя, вступившие с Организацией в договорные отношения.

Персональные данные Клиента – информация, необходимая Оператору в связи с договорными отношениями или благотворительной деятельностью и касающаяся конкретного Клиента, в том числе его фамилия, имя, отчество; год, месяц, дата и место рождения; сведения о трудовом и общем стаже; имущественное положение; семейное положение, сведения о составе семьи; статус семьи; паспортные данные; данные миграционной карты; данные патента на работу; данные разрешения на временное пребывание или проживание, данные вида на жительство иностранного гражданина; сведения о воинском учете; налоговый статус (резидент/нерезидент); сведения о доходах; реквизиты банковского счета, карты; сведения о социальных льготах; образование; профессия; специальность; адрес места жительства; телефон; адрес электронной почты; место работы и/или учебы; место работы или учебы членов семьи и родственников; содержание Договора с оператором; информация, содержащуюся в страховом свидетельстве обязательного пенсионного страхования, свидетельстве о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации, страховом медицинском полисе обязательного медицинского страхования граждан, сведения о наличии/отсутствии у

гражданина заболевания(-ий), препятствующего получения услуг от Оператора; интересы, увлечения, хобби; все аналогичные сведения его родителей/законных представителей иные сведения указанные заявителем.

Персональные данные Контрагента – информация, необходимая Оператору в связи с договорными отношениями и касающаяся конкретного Контрагента, в том числе фамилия, имя, отчество; год, месяц, дата и место рождения; сведения о трудовом и общем стаже; семейное положение, сведения о составе семьи; паспортные данные; данные миграционной карты; данные патента на работу; данные разрешения на временное пребывание или проживание, данные вида на жительство иностранного гражданина; сведения о воинском учете; налоговый статус (резидент/нерезидент); реквизиты банковского счета, карты; сведения о социальных льготах; образование; профессия; специальность; адрес места жительства; телефон; адрес электронной почты; содержание договора с Оператором; содержание декларации, подаваемой в налоговую инспекцию; информация, содержащаяся в страховом свидетельстве обязательного пенсионного страхования, свидетельство о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации, иные сведения указанные заявителем.

Персональные данные Работника - информация, получаемая Оператором, в качестве работодателя, в связи с трудовыми отношениями и касающаяся конкретного работника. Под информацией о работниках понимаются сведения о фактах, событиях и обстоятельствах жизни работника, позволяющие идентифицировать его личность, в том числе: фамилия, имя, отчество; год, месяц, дата и место рождения; сведения о трудовом и общем стаже; семейное положение, сведения о составе семьи; паспортные данные; данные миграционной карты; данные патента на работу; данные разрешения на временное пребывание или проживание, данные вида на жительство иностранного гражданина; сведения о воинском учете; налоговый статус (резидент/нерезидент); сведения о заработной плате работника; реквизиты банковского счета, карты; сведения о социальных льготах; образование; профессия; специальность; занимаемая должность; адрес места жительства; телефон; адрес электронной почты; место работы или учебы членов семьи и родственников; содержание трудового договора; состав декларируемых сведений о наличии материальных ценностей; содержание декларации, подаваемой в налоговую инспекцию; иную, не указанную выше информацию, содержащуюся в личных делах и трудовых книжках сотрудников; информацию, являющуюся основанием к приказам по личному составу; информацию, содержащуюся в страховом свидетельстве обязательного пенсионного страхования, свидетельство о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации, страховом медицинском полисе обязательного медицинского страхования граждан, сведения о наличии/отсутствии у гражданина заболевания(-ий), препятствующего поступлению на работу в Организацию; дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям иные сведения указанные заявителем.

Персональные данные Добровольца - информация, необходимая Оператору, в связи с договорными отношениями в области добровольческой деятельности и касающаяся конкретного добровольца, в том числе: фамилия, имя, отчество; год, месяц, дата и место рождения; сведения о трудовом и общем стаже; семейное положение, сведения о составе семьи; паспортные данные; данные миграционной карты; данные разрешения на временное пребывание или проживание, данные вида на жительство иностранного гражданина; сведения о воинском учете; налоговый статус (резидент/нерезидент); реквизиты банковского счета, карты; сведения о социальных льготах; образование; профессия; специальность; адрес места жительства; телефон; адрес электронной почты; содержание договора с Оператором; информация, содержащаяся в страховом свидетельстве обязательного пенсионного страхования, свидетельство о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации, сведения о наличии/отсутствии у гражданина заболевания(-ий), препятствующего осуществления конкретной добровольческой

деятельности, место работы и/или учебы, интересы, увлечения, хобби, иные сведения указанные заявителем.

Персональные данные, разрешенные субъектом персональных данных для распространения - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом «О персональных данных».

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Субъект персональных данных – Работник, Доброволец, Клиент, Контрагент.

Задача персональных данных Работника, Добровольца, Клиента, Контрагента – деятельность Организации по обеспечению с помощью локального регулирования порядка обработки персональных данных и организационно-технических мер конфиденциальности информации.

Конфиденциальность персональных данных – обязательное для соблюдения лицом, получившим доступ к персональным данным, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Информационная система персональных данных (ИСПД) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.4. Персональные данные работников Организации относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законодательством Российской Федерации.

1.5. Действия настоящего Положения распространяется на всех Работников, Добровольцев, Клиентов и Контрагентов Организации.

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. В целях обеспечения прав и свобод человека и гражданина Организация и (или) его представители при обработке персональных данных должны соблюдать следующие общие требования:

2.1.1. Обработка персональных данных должна осуществляться на законной и справедливой основе, исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия выполнения договорных обязательств в соответствии с законодательством РФ;

2.1.2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.1.3. Получение Организацией персональных данных может осуществляться как путем представления их самим работником, Добровольцем, клиентом, контрагентом так и путем получения их из иных источников.

2.1.4. Персональные данные получаются Организацией непосредственно у самого работника, добровольца, клиента, контрагента. Если персональные данные работника возможно получить только у третьей стороны, то субъект персональных данных должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Организация должна сообщить субъекту персональных данных о целях, предполагаемых источниках и способах

получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа дать письменное согласие на их получение.

2.1.5. Организация не имеет права получать и обрабатывать персональные данные работника, добровольца, клиента, контрагента о его расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, кроме случаев, прямо предусмотренных Федеральным законом.

2.2. К обработке, передаче и хранению персональных данных могут иметь доступ:

- Президент Организации
- Директора Организации по направлению деятельности (доступ к личным данным только сотрудников, добровольцев, клиентов и контрагентов своей программы, проекта);
- Координаторы программ, направлений деятельности, проектов в своем подразделении (доступ к личным данным только сотрудников, добровольцев, клиентов и контрагентов своего подразделения);
- при переводе из одного структурного подразделения в другое доступ к персональным данным сотрудника, добровольца может иметь руководитель/координатор нового подразделения;
- сам Субъект, источник персональных данных;
- другие сотрудники Организации при выполнении ими своих служебных обязанностей на основании должностных обязанностей и инструкций.

2.3. Использование персональных данных возможно только в соответствии с целями, определившими их получение.

Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено действующим законодательством Российской Федерации.

2.4. При принятии решений, затрагивающих интересы клиента или контрагента, Оператор не имеет права основываться на персональных данных клиента или контрагента, полученных исключительно в результате их автоматизированной обработки без его письменного согласия на такие действия.

2.5. При идентификации клиента или контрагента Организация может потребовать представления документов, удостоверяющих личность и подтверждающих полномочия представителя.

2.6. При заключении договора, как и в ходе выполнения договора может возникнуть необходимость в предоставлении клиентом или контрагентом иных документов, содержащих информацию о нем.

2.7. После принятия решения о заключении договора или представления документов, подтверждающих полномочия представителя, а также впоследствии, в процессе выполнения договора, содержащего персональные данные клиента или контрагента, к документам, связанным с исполнением договора, содержащего персональные данные клиента, также могут относиться:

- договоры;
- приказы по основной деятельности;
- служебные записки;
- приказы о допуске к персональным данным представителей клиента, контрагента;
- разовые или временные пропуска;
- другие документы, где включение персональных данных клиента или контрагента необходимо согласно действующему законодательству.

2.8. Передача персональных данных возможна только с согласия работника, добровольца, клиента, контрагента или в случаях, прямо предусмотренных законодательством Российской Федерации.

2.8.1. При передаче персональных данных Организация должна соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия работника, добровольца, клиента, контрагента за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, клиента, контрагента, а также в случаях, установленных законодательством Российской Федерации;

- не сообщать персональные данные в коммерческих целях без его письменного согласия; предупредить лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными в порядке, установленном законодательством Российской Федерации; разрешать доступ к персональным данным, только специально уполномоченным лицам, определенным Приказом Организации, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

- передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

2.8.2. Передача персональных данных от Организации и (или) его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

2.8.3. При передаче персональных данных внешним потребителям (в том числе и в коммерческих целях) Организация не должна сообщать эти данные третьей стороне без письменного согласия работника, добровольца, клиента, контрагента за исключением случаев, установленных законодательством Российской Федерации.

2.9. Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

2.10. Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

2.11. Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

2.12. Период хранения и обработки персональных данных определяется в соответствии с Законом «О персональных данных». Обработка персональных данных начинается с момента поступления персональных данных в информационные системы персональных данных.

2.13. Оператор персональных данных обязан:

2.13.1. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов

персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

2.13.2. В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

2.13.3. В случае выявления неправомерной обработки персональных данных, осуществляющейся оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные или обеспечить их уничтожение. Об устраниении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

2.13.4. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

2.13.5. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях,

предусмотренных Федеральным законом «О персональных данных» или другими федеральными законами.

2.13.6. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 2.13.3 – 2.13.5 настоящего Положения, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

2.13.7. Прекратить обработку персональных данных в случае прекращения деятельности Организации.

2.14. Оператор вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных, если иное не предусмотрено федеральным законом, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее - поручение оператора). Лицо, осуществляющее обработку персональных данных по поручению оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом -ФЗ «О персональных данных». В поручении оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

2.15. В случае, если оператор поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет оператор. Лицо, осуществляющее обработку персональных данных по поручению оператора, несет ответственность перед оператором.

2.16. Особенности обработки персональных данных, разрешенных субъектом персональных данных для распространения

2.16.1. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных. Оператор обязан обеспечить субъекту персональных данных возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2.16.2. Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения, может быть предоставлено оператору: 1) непосредственно; 2) с использованием информационной системы уполномоченного органа по защите прав субъектов персональных данных.

2.16.3. Субъект персональных данных вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных субъектом персональных данных для распространения, к Организации. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) субъекта персональных данных, а также перечень персональных данных, обработка которых подлежит прекращению. Организация обязана прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования субъекта персональных данных или в срок, указанный во вступившем в законную силу решении суда, а

если такой срок в решении суда не указан, то в течение трех рабочих дней с момента вступления решения суда в законную силу.

3. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

3.1. ВНУТРЕННИЙ ДОСТУП

3.1.1. Список лиц, допущенных к обработке персональных данных (далее Список) и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение правил обработки персональных данных, определяется и утверждается Приказом.

3.1.2. Подразделение по работе с персоналом при принятии на работу, увольнении или изменении должностных обязанностей Работников не позднее чем в трехдневный срок вносит изменения в Список лиц, допущенных к обработке персональных данных.

3.1.3. Работники Организации выполняют действия по обработке персональных данных в соответствии с возложенными на работников функциями.

3.1.4. Доступ к персональным данным предоставляется только лицам, замещающим должности из Списка. Работа с ИСПДн осуществляется в соответствии с «Инструкцией пользователя информационной системы персональных данных».

3.1.5.. Работники имеют доступ на ввод и коррекцию персональных данных в пределах, определенных должностными обязанностями.

3.1.6. Лица, получившие доступ к персональным данным, должны хранить в тайне известные им сведения конфиденциального характера и информировать Ответственного за ООПД об утечке персональных данных, о фактах нарушения порядка обращения с ними, о попытках несанкционированного доступа к персональным данным.

3.1.7. Лица, получившие доступ к персональным данным, должны использовать эти данные лишь в целях, для которых они сообщены, обязаны соблюдать режим конфиденциальности и дать Обязательство о конфиденциальности и неразглашении персональных данных (Приложение №1). Руководители структурных подразделений имеют право ознакомиться с документами, содержащими персональные данные подчиненного им работника, в помещении отдела кадров в присутствии сотрудника, ответственного за работу с соответствующими документами.

3.1.8. Работник имеет право ознакомиться с документами, содержащими его персональные данные, в помещении отдела кадров в присутствии сотрудника, ответственного за работу с соответствующими документами.

3.2. ВНЕШНИЙ ДОСТУП.

3.2.1. Передача информации третьей стороне возможна только при письменном согласии работников.

3.2.2. К лицам, которым могут быть переданы персональные данные вне организации, при условии соблюдения требований законодательства, относятся:

- налоговые инспекции;
- правоохранительные органы;
- органы статистики;
- страховые агентства;
- военкоматы;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

3.2.3. Надзорно-контрольные органы имеют доступ к информации только в сфере своей компетенции.

3.2.4. Организации, в которые сотрудник может перечислять денежные средства (страховые компании, негосударственные пенсионные фонды, благотворительные организации,

кредитные учреждения), могут получить доступ к персональным данным работника только при наличии его письменного разрешения.

3.2.5. Сведения о работающем или уволенном работнике могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии или оригинала нотариально заверенного заявления работника.

3.2.6. Персональные данные работника могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого работника.

4. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию. Риск угрозы любым персональным данным создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

4.2. Защита персональных данных представляет собой процесс, предупреждающий нарушение целостности, достоверности и конфиденциальности персональных данных и в конечном счете обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности организации.

4.3. Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств и в порядке, установленном федеральным законом.

4.4. Защите подлежит:

- информация о персональных данных субъекта;
- документы, содержащие персональные данные субъекта;
- персональные данные, содержащиеся на электронных носителях.

4.5. ВНУТРЕННЯЯ ЗАЩИТА

4.5.1. Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать следующие меры:

- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором, исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно-методических документов по защите информации и сохранению тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава работников, имеющих право доступа к персональным данным работников;
- организация процесса уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения; разъяснительная работа с сотрудниками подразделения, цель которой – предупредить утрату ценных сведений при работе с персональными данными.

4.5.2. Выдача документов на бумажном носителе, содержащих персональные данные работника, на рабочие места руководителей структурных подразделений запрещена.

4.6. ВНЕШНЯЯ ЗАЩИТА

4.6.1. Для защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить

несанкционированный доступ к персональным данным работника. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только получение сведений и их использование, но и их видоизменение, уничтожение, подмена, фальсификация содержания документа и др.

4.6.2. Распределение функций, рабочих процессов, технологий составления, оформления, ведения и хранения документов, содержащих персональные данные работника, в Организации является закрытой от посторонних лиц информацией.

*Под посторонним лицом понимается любое лицо, в чей функционал не входит доступ к персональным данным.

4.7. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Зашита персональных данных в информационной системе обеспечивается 3-им уровнем защищенности персональных данных:

- организован режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечивается сохранность носителей персональных данных;
- руководителем Организации утвержден перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

4.8. Все лица, в должностные обязанности которых входит получение, обработка и защита персональных данных работника, при приеме на работу обязаны подписать обязательство о конфиденциальности и неразглашении персональных данных работника.

4.9. Работники, клиенты или контрагенты до предоставления своих персональных данных должны иметь возможность ознакомиться с настоящим Положением.

4.10. Оператор издает документы, определяющие политику оператора в отношении обработки персональных данных, локальные акты по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

4.11. Оператор принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных в соответствии со статьей 19 Федерального закона «О персональных данных».

4.12. Оператор обеспечивает ознакомление своих работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников;

4.13. Ответственные лица соответствующих подразделений, хранящих персональные данные на бумажных носителях и машинных носителях информации, обеспечивают их защиту от несанкционированного доступа и копирования согласно «Положению об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации», утвержденному Постановлением правительства РФ 15 сентября 2008 г. N 687.

4.14. Ответственные лица подразделений, обрабатывающие персональные данные, в информационных системах персональных данных и машинных носителях информации, обеспечивают защиту в соответствии с Постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативными, нормативно-методическими, методическими документами.

4.15. По возможности персональные данные должны быть обезличены.

4.16. Обеспечение безопасности персональных данных, а также разработка и внедрение средств защиты персональных данных основывается на анализе угроз безопасности персональных данных.

5. ПРАВА И ОБЯЗАННОСТИ РАБОТНИКА

5.1. Работники и их представители должны быть ознакомлены под расписку с документами Организации, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

5.2. В целях защиты персональных данных, хранящихся у работодателя, работник имеет право:

5.2.1. Требовать уточнения, исключения или исправления неверных или неполных персональных данных;

5.2.2. На свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные этого работника;

5.2.3. Персональные данные оценочного характера дополнить заявлением, выражающим его собственную точку зрения;

5.2.4. Определять своих представителей для защиты своих персональных данных;

5.2.5. На сохранение и защиту своей личной и семейной тайны.

5.2.6. Получать от работодателя:

- сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
- перечень обрабатываемых персональных данных и источник их получения;
- сроки обработки персональных данных, в том числе сроки их хранения;

5.2.7. Требовать извещения работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные работника, обо всех произведенных в них исключениях, исправлениях и дополнениях;

5.2.8. Обжаловать в суде любые неправомерные действия или бездействия работодателя при обработке и защите его персональных данных;

5.2.9. В целях защиты частной жизни, личной и семейной тайны работники вправе отказываться от обработки таких персональных данных без их согласия; Иные права, предоставленные законом.

5.3. Работник обязан:

5.3.1. передавать Организации и (или) его представителю комплекс достоверных, документированных персональных данных, состав которых установлен Трудовым кодексом Российской Федерации. 5.3.2. В трехдневный срок сообщать в Организацию об изменении своих персональных данных: фамилии, имени, отчества, даты рождения, что получает отражение в трудовой книжке на основании представленных документов. При необходимости изменяются данные об образовании, профессии, специальности, присвоении нового разряда и пр.

6. ПРАВА И ОБЯЗАННОСТИ ДОБРОВОЛЬЦЕВ, КЛИЕНТОВ И КОНТРАГЕНТОВ

6.1. В целях обеспечения защиты персональных данных, хранящихся у Оператора, клиенты, добровольцы и контрагенты имеют право на:

6.1.1. Полную информацию о составе персональных данных и их обработке, в частности доброволец, клиент или контрагент имеет право знать, кто и в каких целях использует или использовал информацию о его персональных данных.

6.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные добровольца, клиента или контрагента, за исключением случаев, предусмотренных законодательством РФ.

6.1.3. Определение своих представителей для защиты своих персональных данных.

6.1.4. Требование об исключении или исправлении неверных или неполных устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Оператора персональных данных. При отказе Оператора исключить или исправить персональные данные клиента или контрагента он имеет право заявить в письменной форме Оператору о своем несогласии с соответствующим обоснованием такого несогласия.

6.1.5. Требование об извещении Оператором всех лиц, которым ранее были сообщены неверные или неполные персональные данные добровольца, клиента или контрагента, обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.1.6. Обжалование в суд любых неправомерных действий или бездействия Оператора при обработке и защите его персональных данных.

6.2. В целях обеспечения достоверности персональных данных, доброволец, клиент и контрагент обязан:

6.2.1. При заключении договора предоставить Оператору полные и достоверные данные о себе;

6.2.2. В случае изменения сведений, составляющих персональные данные добровольца, клиента или контрагента, незамедлительно, но не позднее трех рабочих дней, предоставить данную информацию Оператору.

7. ОРГАНИЗАЦИЯ ВНУТРЕННЕГО КОНТРОЛЯ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Цели организации внутреннего контроля

7.1.1. Организация внутреннего контроля процесса обработки персональных данных в Организации осуществляется в целях изучения и оценки фактического состояния защищенности персональных данных, своевременного реагирования на нарушения установленного порядка их обработки, а также в целях совершенствования этого порядка и обеспечения его соблюдения.

7.1.2. Мероприятия по осуществлению внутреннего контроля обработки и обеспечения безопасности персональных данных направлены на решение следующих задач:

- обеспечение соблюдения работниками Оператора требований настоящего Положения и нормативных правовых актов, регулирующих защиту персональных данных;
- оценка компетентности персонала, задействованного в обработке персональных данных;

- обеспечение работоспособности и эффективности технических средств информационных систем персональных данных и средств защиты персональных данных, их соответствия требованиям уполномоченных органов исполнительной власти по вопросам безопасности персональных данных;
- выявление нарушений установленного порядка обработки персональных данных и своевременное предотвращение негативных последствий таких нарушений;
- принятие корректирующих мер, направленных на устранение выявленных нарушений, как в порядке обработки персональных данных, так и в работе технических средств информационных систем персональных данных;
- разработка рекомендаций по совершенствованию порядка обработки и обеспечения безопасности персональных данных по результатам контрольных мероприятий;
- осуществление контроля за исполнением рекомендаций и указаний по устраниению нарушений.

7.2. Проведение контрольных мероприятий:

7.2.1. Ответственный за организацию обработки персональных данных на периодической основе (не реже одного раза в три года) организует проведение внутреннего контроля соблюдения порядка обработки и обеспечения безопасности персональных данных.

7.2.2. Проведение контрольных мероприятий по обеспечению безопасности персональных данных должно включать:

- проведение проверок деятельности работников Оператора, допущенных к работе с персональными данными в информационных системах персональных данных, на соответствие порядку обработки и обеспечения безопасности персональных данных, установленному настоящим Положением, ФЗ «О персональных данных» и другими нормативными правовыми актами;
- проверку правильности приема и обработки обращений и запросов субъектов персональных данных или их представителей;
- проведение проверок состояния защищенности персональных данных, обрабатываемых в информационной системе персональных данных, включая проверку доступов пользователей к персональным данным, выполнение требований по защите каждой конкретной информационной системе, корректности работы системы защиты персональных данных и т. д.

7.2.3. Все результаты проверок должны быть предоставлены Оператору для проведения анализов результатов и принятия мер по обеспечению безопасности персональных данных.

При необходимости должны быть предложены меры по минимизации последствий выявленных угроз информационных систем.

7. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СВЯЗАННОЙ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ РАБОТНИКОВ

7.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

7.2. Руководство Оператора несет ответственность за обеспечение конфиденциальности,

целостности и доступности персональных данным, а также соблюдение прав и свобод субъектов персональных данных в отношении их персональных данных, в том числе прав на неприкосновенность частной жизни, личную и семейную тайну.

7.3. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

7.4. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

7.5. Каждый сотрудник организации, получающий для работы конфиденциальный документ, несет персональную ответственность за соблюдение требований по обработке и обеспечению безопасности персональных данных, сохранность носителя и конфиденциальность информации, установленных настоящим Положением, в соответствии с законодательством Российской Федерации

7.6. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

7.6.1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него обязанностей по соблюдению установленного порядка работы со сведениями конфиденциального характера Организация вправе применять предусмотренные Трудовым кодексом Российской Федерации дисциплинарные взыскания.

7.6.2. Должностные лица, в обязанность которых входит обработка персональных данных, обязаны обеспечить каждому Клиенту возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом. Неправомерный отказ в предоставлении собранных в установленном порядке документов, либо несвоевременное предоставление таких документов или иной информации в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации - влечет наложение на должностных лиц административного штрафа в размере, определяемом Кодексом об административных правонарушениях.

7.6.3. В соответствии с Гражданским кодексом лица, незаконными методами получившие информацию, составляющую служебную тайну, обязаны возместить причиненные убытки, причем такая же обязанность возлагается и на работников.

7.6.4. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения наказывается в соответствии с законодательством Российской Федерации.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1 Настоящее Положение вступает в силу с момента его утверждения Приказом руководителя.

8.2 Настоящее Положение доводится до сведения всех работников Организации персонально под роспись.

8.3. Неотъемлемой частью настоящего положения являются следующие Приложения:

8.3.1. Приложение №1. Обязательство сотрудника о конфиденциальности и неразглашении персональных данных

ОБЯЗАТЕЛЬСТВО
о конфиденциальности и неразглашении персональных данных

Я,

(фамилия, имя, отчество)

Обязуюсь, получая доступ к персональным и биометрическим данным работников АНО «Новые перспективы», обладающим потенциальной ценностью в силу их неизвестности третьим лицам, которые могли бы получить выгоду от разглашения или использования персональных и биометрических данных, не передавать или разглашать эти данные третьим лицам:

- фамилия имя отчество сотрудников;
- паспортные данные;
- домашние адреса;
- телефоны сотрудников;
- места прежней работы;
- телефоны родственников;
- состав семьи и семейное положение;
- информацию о моральных и деловых качествах;
- возраст;
- образование;
- состояние здоровья;
- сведения о заработной плате сотрудников;
- сведения о руководителях организаций.

В случае попытки третьих лиц получить от меня информацию о персональных данных сотрудников или руководства, обязуюсь сообщить незамедлительно о данном факте, с указанием этого третьего лица непосредственному руководителю или директору организации.

Информация не будет обладать признаком конфиденциальности, и я не буду иметь никаких обязательств в отношении данной информации, если последняя удовлетворяет одному из следующих пунктов:

- 1) представлена третьей стороне руководством Организации или уполномоченным лицом;
- 2) разрешена к выпуску письменным разрешением (приказом) руководства Организации;
- 3) раскрыта правительству по требованию правительенного органа, основанному на законодательстве РФ.
- 4) раскрыта по требованию официальных органов, государственных служб и ведомств на законном основании.

Я предупрежден(а), что буду ответственен(а) за умышленное или неумышленное разглашение или использование персональных данных, если бы в отношении своих собственных персональных данных аналогичной важности соблюдал(а) осторожность, и если бы после обнаружения умышленного или неумышленного разглашения или использования персональных данных я не прекратил(а) их умышленное или неумышленное разглашение или использование.

Я предупрежден(а), что в случае нарушения этого Обязательства, буду нести дисциплинарную ответственность вплоть до увольнения с работы по пункту б (в) части первой статьи 81 Трудового Кодекса Российской Федерации, а также предусмотренную в соответствии с Законодательством Российской Федерации административную и уголовную ответственность в соответствии со статьей 137 Уголовного Кодекса Российской Федерации.